身份认证

2020年5月19日 22:43

-
- 身份认证

1. 身份认证：验证主体的真实身份与其所声称的身份是否符合的过程
    a. 认证的结果：符合、不符合
    b. 适用于用户、进程、系统、信息等
2. 身份认证系统
    a. 出示证件的人，称作示证者P(Prover)，又称声称者(Claimant)
    b. 验证者V（Verifier)，检验声称者提出的证件的正确性和合法性，决定是否满足要求
    c. 第三方是可信赖者TP（Trusted third party)，参与调解纠纷。在许多应用场合下没有第三方
3. 身份认证物理基础
    a. 用户所知道的(Something the user know, 例如口令)
        i. 简单，但不安全
        ii. 指用户心里知道的一些东西。可能是一个口令，或用户和认证者共享的一个机密字
        iii. 注意“弱密钥”
        iv. 使用一次性密钥。如网上银行业务
        v. 设计依据：安全水平、系统通过率、用户可接受性、成本等
    b. 用户所拥有的(Something the user possesses, 例如证件)
        i. 指用户获取的关于身份识别的各种物理实体，如安全内核，动态口令卡，安全暗号，或者其他任何形式的卡或标签
        ii. 认证系统相对复杂
    c. 用户所特有的(Something the user is,例如指纹识别)
        i. 更复杂,而且有时会牵涉到本人意愿
        ii. 指用户本身特有的生物特征，比如声音，指纹，虹膜，DNA等其他一些生物特征
        iii. 指纹识别、虹膜识别、人脸识别、掌纹识别、声音识别、签名识别、笔迹识别、手形识别、步态识别等
4. 身份认证方式
    a. 单向认证（One-way Authentication）：通信的一方认证另一方的身份
        i. 基于对称密码体制：A发送加密后的随机数R，B回复对R所对应的某函数值加密后得到的值
        ii. 基于非对称密码体制：A发送随机数R，B回复私钥K_SB加密后的A
    b. 双向认证（Two-way Authentication）：双方都要提供用户名和密码给对方
        i. 基于对称密码体制：A发送加密后的随机数R_A，B回复加密后的R_A||随机数

R_B，A再发送加密后的R_B

ii. 基于非对称密码体制：A发送随机数R_A，B回复用B的私钥K_SB加密后的R_A||随机数R_B，A再发送用A的私钥K_SA加密后的R_B

c. 信任的第三方认证（Trusted Third-party Authentication）：通信双方连线前先彼此通过信任第三方的认证，然后才能互相交换密钥，而后进行通信

i. 如：从密钥分发中心KDC（Key Distribution Center）获得对方公钥

ii. 如：Kerberos分布式认证服务